Volume 15, Issue 18   Atari Online News, Etc.   May 10, 2013

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1518   05/10/13

~ Cern Recreating First! ~ Cyberwar Strategies?   ~ Teens vs. Adults?

-* New Law To Combat Cyber Theft *-
-* No Internet? Next Xbox Still Works! *-
-* Internet Sales Tax Bill, Tough House Sell! *-

=~=~=~=

->From the Editor’s Keyboard   "Saying it like it is!"
""""""""""""""""""""""""""""

First off, I want to apologize for the lack of an issue last week. During the entire week, I was tied up dealing with my father’s estate which ended up culminating in a trip to Maine which took up most of the day Friday. It was a long week, and an extremely long day! There was no way that I was going to complete the week’s issue, nor even get tt done late. So, we’re back this week.

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Next Xbox Will Work Even When Your Internet Doesn t!
""""""""""""""""""""""""""""""   Ouya Delayed to End of June!
Call of Duty: Ghost Coming!
And much more!

=~=~=~=

->A-ONE’s Game Console Industry News   - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Microsoft: Next Xbox Will Work Even When Your Internet Doesn t

Should single-player games, Blu-ray playback, and live TV viewing be possible on a gaming console with no Internet connection? Most gamers would say "yes," but they have been worried that Microsoft feels differently; the next generation Xbox has been consistently rumored to require a permanent network connection.

It won’t.

According to an internal Microsoft e-mail sent to all full-time employees working on the next Xbox, "Durango [the codename for the next Xbox] is designed to deliver the future of entertainment while engineered to be tolerant of today’s Internet." It continues, "There are a number of scenarios that our users expect to work without an Internet connection, and those should ’just work’ regardless of their current connection status. Those include, but are not limited to: playing a Blu-ray disc, watching live TV, and yes playing a single player game."

The quotation also implicitly confirms another rumor: the next Xbox will sport an HDMI input, to allow cable boxes to be hooked up for live TV viewing. Our sources tell us that the console will be able to provide TV listings and similar information.

How far this offline support will extend still isn’t clear. It could take the form of a fully offline mode akin to that on the Xbox 360 (insert optical disc, install game, play, all without an Internet connection) or it could be more like Steam (install and activate online but enable subsequent offline play once this has been done).

While one could argue that "installing a game" is one of the "scenarios" that gamers "expect to work" when offline, a more Steam-like approach would be consistent with rumors that the next Xbox will use its Internet connection to block installation of secondhand games.

Still, though the next Xbox won’t make everybody happy, it looks like fears that the console will be useless when your broadband goes down have been overblown.

Ouya Delayed to End of June, Snatches $15 Million in New Funding

The most visible of the Android-based micro-consoles with the name that sounds like what Kool-Aid man says when he s busting through painted styrofoam walls will delay its $100 Ouya game cube until the end of June: specifically June 25   about two weeks after E3 wraps.

The reason for the delay? The company doesn t say in a press release that s mostly about other stuff, burying the revised launch date at the end (the system was originally due out June 4), but Joystiq managed to speak with Ouya honcho Julie Uhrman, who explains the sudden pushback:

We ve had incredibly positive reactions from our retail partners, and so in order to meet their greater than expected demand, we decided to shift the launch date by a couple of weeks   three weeks   which will allow us to create more units and, basically, have more units on store shelves in June.

You know all the worry about the controller feeling cheap? Complaints about some of the buttons sticking under the top plate when hammered? It sounds like Ouya s already addressed this (well, the button-sticking part anyway): Uhrman says the company s made the holes for the face buttons a trifle larger to rectify the problem. We made that change very early so all the units are being produced with those larger button holes, says Uhrman. The revised controllers are already shipping to Kickstarter backers.

As Gamasutra notes, the new launch date pits Ouya squarely against

GameStick, a flash drive-sized, Android-based game console designed to plug directly into Smart TVs (or to a standard TV through an HDMI dock). GameStick has a launch date of June 10, but the company s said the first units won t be in the hands of those who preordered it until the final week of June.

But what Ouya really wants everyone to know, is that it just secured $15 million in new funding led by Silicon Valley-based venture capital firm Kleiner Perkins Caufield & Byers, with participation from Mayfield Fund, NVIDIA, Shasta Ventures and Occam Partners. If KPCB rings some distant game history bells, it may be because it s the company EA Chief Creative Officer Bing Gordon joined upon leaving Electronic Arts in 2008. Gordon originally signed up with EA in 1982 (just a few months after its inception), devoting over a quarter century to the game giant Trip Hawkins started. As part of the Ouya funding deal, Gordon will join Ouya s board of directors alongside Uhrman as well as Roy Bahat, chairman of the board (Gordon also serves on the board of directors at Amazon, Klout, Lockerz, MEVIO, Zazzle and Zynga).

Ouya raised nearly $8.6 million last summer, with over 63,000 Kickstarter backers throwing in to propel the conceptual console well beyond its stated $950,000 goal. Preliminary reviews of initial beta systems dispatched to backers in late March have been mixed, spawning a handful of apologias. No, Kickstarter projects aren t by necessity grab something and hang on! beta pilgrimages   Nataly Dawn s Kickstarter-funded album How I Knew Her sounds like something that cost a lot more than $100k to produce, and for my money, games column Tom vs. Bruce (also Kickstarter-funded) is absolutely peerless   but yes, it s true, mass-manufactured technology with ergonomic variables and questionable launch software lineups rarely arrive blemish-free.

In any event, Ouya s real challenge isn t pricing ($100 is plenty cheap) or patching up gamepad glitches (already well in hand) or whether this button should have been here or there, it s about what this thing s going to let you do when you power it on. No one cares about the aesthetics (it s a grayish plastic cube, so what), and you have to try pretty hard at this point to screw up a gamepad with conventional face buttons, thumbsticks and triggers. But if Ouya launches with a stable of been-there-played-that games, well will gamers leap in for the fiddly emulators and tiny handful of media services, all for the elusive promise of better to come? That s the $8.6 million dollar question.

Call of Duty: Ghost Coming to Xbox 360, PS3, PC and Next-gen Platforms

Activision on Wednesday announced that the latest installment of its best-selling Call of Duty franchise, called Call of Duty: Ghost, will launch later this year on the Xbox 360, PlayStation 3, PC and next generation platforms. The latest Call of Duty game is being developed by Infinity Ward, the studio behind the original Call of Duty and the critically acclaimed Call of Duty: Modern Warfare series. Activision s first-person shooter has consistently shattered game sale records year after year and its latest installment is expected to continue this trend. Call of Duty: Ghost is scheduled to be released on November 5th. Starting today, fans can pre-order the game at retail stores. Activision s press release follows below.

ACTIVISION ANNOUNCES THE NEXT GENERATION OF CALL OF DUTY WITH CALL OF DUTY:

GHOSTS

Call of Duty: Ghosts will set a new Benchmark for the Next Generation

All-New World, Story, Characters and Experience, All Powered by New, Next Gen Call of Duty Engine from the Developer that started it all, Infinity Ward

For an Exclusive First Look at the Game, Tune in to Xbox: The New Generation Revealed, May 21 at 10AM PDT on Xbox.com, Xbox Live or SPIKE TV

Groundbreaking Title Lands on November 5

Santa Monica, CA   May 1, 2013   Prepare for the next generation of Call of Duty. The franchise that has defined a generation of gaming is set to raise the bar once again with the all-new Call of Duty: Ghosts. Published by Activision Publishing, Inc., a wholly owned subsidiary of Activision Blizzard, and developed by Infinity Ward, the studio that created the original Call of Duty and the seminal Call of Duty: Modern Warfare series, Call of Duty: Ghosts ushers in the next generation of the franchise. The new title delivers a riveting all-new gameplay experience built on an entirely new story, setting and cast of characters, all powered by a new, next generation Call of Duty engine that redefines the series for the next generation.

Infinity Ward set the gold standard for first-person action for a generation, and they re going to do it again with Call of Duty: Ghosts, said Eric Hirshberg, CEO of Activision Publishing, Inc. Ghosts delivers an all-new story, all-new characters, an all-new Call of Duty world, all powered by a next generation Call of Duty engine, which is a leap forward for the franchise. Infinity Ward is going all-in to create the next generation of Call of Duty worthy of the world s greatest fans.

Everyone was expecting us to make Modern Warfare 4, which would have been the safe thing to do. But we re not resting on our laurels, said Mark Rubin, executive producer of developer Infinity Ward. We saw the console transition as the perfect opportunity to start a new chapter for Call of Duty. So we re building a new sub-brand, a new engine, and a lot of new ideas and experiences for our players. We can t wait to share them with our community.

To see an exclusive first look at Call of Duty: Ghosts tune in to Xbox: the Next Generation Revealed on May 21 at 10AM PDT on Xbox.com, Xbox LIVE or SPIKE TV for the debut of the all-new game from Infinity Ward.

We are consistently thrilled with the overwhelming response received from critics and consumers alike to the Call of Duty series, which has firmly established its home on the Xbox 360 with the game s largest and most engaged community, said Don Mattrick, president of the interactive entertainment business at Microsoft. With Call of Duty: Ghosts, we have no doubt that our longtime partners, Activision and Infinity Ward, will raise the bar higher than ever before for this incredible franchise.

Starting today, fans can begin pre-ordering their copy of Call of Duty: Ghosts at retail outlets worldwide.

There s no other video game property like Call of Duty. It s the biggest game franchise on the planet that has had some of the biggest game entertainment launches in history, said Tony Bartel, president of GameStop. We are very excited for the launch of Call of Duty: Ghosts, as we transition to next generation consoles.

Call of Duty: Ghosts will release on Xbox 360 video game and entertainment system from Microsoft, PlayStationfi3 computer entertainment system and PC on November 5. Call of Duty: Ghosts will also be available for next generation platforms. For the latest intel, check out: http://www.callofduty.com/ghosts, http://www.facebook.com/CODGhosts, or follow on Twitter @InfinityWard. Call of Duty: Ghosts is not yet rated.

GameStop Ending PlayStation 2 Trade-Ins in June

GameStop has confirmed that it will no longer accept PlayStation 2 trade-ins as of June 1, 2013. In a statement provided to IGN, a GameStop representative said the following:

We can confirm that as of June 1st we will no longer be accepting the PS2 console or its related product for trades. We know that the 12 year old system is a popular one and for many gamers, GameStop is the only place to find a great selection of its games. We will still offer a wide selection of the PS2 hardware, accessories and games in many of our stores and online for several months, based on remaining stock from trades.

We are very excited about the upcoming PS4 and are making room in our stores for it and other new platforms expected this fall.

Earlier this year, Sony ceased production of the PlayStation 2, ending its life as the best-selling home console of all time. Since its launch in 2000, more than 150 million PlayStation 2s have been sold worldwide, with more than 1.5 billion software units sold.

Video Game Play Sharpens Elderly Minds

Wanna help grandma keep her mind sharp? Consider throwing out her crossword puzzles and giving her a joystick. Because a study finds that elderly people who played a video game for at least 10 hours gained three years of protection from cognitive decline. Gamers also became quicker at processing information. The research is in the journal PLoS ONE. [Fredric D. Wolinsky et al, A Randomized Controlled Trial of Cognitive Training Using a Visual Speed of Processing Intervention in Middle Aged and Older Adults]

Almost 700 subjects were divided into two groups: those between the ages of fifty and sixty-four and people aged sixty-five and older. Members from each age group were asked to either work on a crossword puzzle or play a video game called Road Tour, which involves matching fleeting images of car types and road signs.

In both age groups, those who played the video game showed improvements on executive function which includes memory, attention, problem solving skills and perception when tested a year later.

Some of the gamers were given four additional hours of training with the game. And their cognitive improvement lasted an additional year. So video games might help ward off cognitive decline. Just don t play Road Tour while actually driving.

Video Game Maker Drops Gun Makers, Not Their Guns

In the midst of the bitter national debate on gun violence, gun manufacturers and videogame makers are delicately navigating one of the more peculiar relationships in American business.

Violent "first-person shooter" games such as "Call of Duty" are the bread and butter of leading video game publishers, and authenticity all but requires that they feature brand-name weapons.

Electronic Arts licensed weapons from companies like McMillan Group International as part of a marketing collaboration for "Medal of Honor: Warfighter." Activision Blizzard gives "special thanks" to Colt, Barrett and Remington in the credits for its "Call of Duty" titles.

Rifles by Bushmaster, which made the gun used in the Newtown, Connecticut school shooting last December, have appeared in the hugely popular "Call of Duty."

Yet, in the wake of the Newtown shooting, the biggest advocate for gun ownership, the National Rifle Association, took aim at videogames to explain gun violence. One week after 20 schoolchildren and six adults were killed in the shooting, NRA chief executive Wayne LaPierre called the videogame industry "a callous, corrupt and corrupting shadow industry that sells, and sows, violence against its own people."

Now at least one game maker, the second largest by revenue in the United States, is publicly distancing itself from the gun industry, even as it finds ways to keep the branded guns in the games. Electronic Arts says it is severing its licensing ties to gun manufacturers - and simultaneously asserting that it has the right, and the intention, to continue to feature branded guns without a license.

For the gunmakers, having their products in games is "free marketing, just like having Coca-Cola" in a movie, said Roxanne Christ, a partner at Latham & Watkins LLP in Los Angeles, who works with video game companies on licensing, but has not personally done a gun deal.

Yet it is also a virtual double-edged sword. "It gives publicity to the particular brand of gun being used in the video game," said Brad J. Bushman, a professor at Ohio State University who has studied video game violence. "On the other hand, it’s linking that gun with violent and aggressive behavior."

Gun makers, including the Freedom Group that owns brands like Remington and Bushmaster, and the NRA, did not respond to repeated requests for comment from Reuters.

First-person shooter games let players blast their way through battlefields while looking down the barrel of a virtual gun, taking aim with the flick of a controller.

Some of those guns - like the Colt M1911 pistol in "Call of Duty" - turn sideways to face the screen during reloading, revealing the brand name. Games also offer lists of branded weapons to choose from.

Licensed images of weapons in "Medal of Honor: Warfighter" - a game that simulates military missions like fighting pirates in Somalia - offer what EA spokesman Jeff Brown calls "enhanced authenticity."

Back in the late 90’s, video game makers initially approached gun companies for licenses to inoculate themselves from potential lawsuits, video game industry lawyers say. Over the years, legal clearances were granted for little or no money by gunmakers, these lawyers said.

Yet overt signs of cooperation between the video game and gun industries had begun to draw criticism even before the December school shooting in Connecticut.

In August, game fans and some video game news outlets vehemently objected to EA putting links to weapons companies like the McMillan Group and gun magazine maker Magpul, where gamers could check out real versions of weapons featured in the game, on its "Medal of Honor: Warfighter" game website.

"What kind of message is a video game publisher like EA sending when it encourages its players to buy weapons?" asked Laura Parker, the associate editor of gaming site GameSpot Australia in a post in August.

EA immediately removed the links and dropped the marketing tie-up, which it said was part of a charity project to raise money for military veterans. The company said it received no money from its gun company partners.

"We won’t do that again," said Brown. "The action games we will release this year will not include licensed images of weapons."

EA said politics and NRA comments critical of game makers had nothing to do with its decision. "The response from our audience was pretty clear: they feel the comments from the NRA were a simple attempt to change the subject," Brown said.

EA also says video game makers can have branded guns in their games without getting licenses, meaning the industry could drop the gun companies and keep their guns.

Activision, the industry leader, declined to comment on whether it licenses gun designs from gun manufacturers or if it would stop doing so. Branded guns have consistently been featured in its blockbuster shooter games like the decade-old "Call of Duty."

"We’re telling a story and we have a point of view," EA’s President of Labels Frank Gibeau, who leads product development of EA’s biggest franchises, said in an interview. "A book doesn’t pay for saying the word ’Colt,’ for example."

Put another way, EA is asserting a constitutional free speech right to use trademarks without permission in its ever-more-realistic games.

Legal experts say there isn’t a single case so far where gun companies have sued video game companies for using branded guns without a license.

But EA’s legal theory is now being tested in court. Aircraft maker Bell Helicopter, a unit of Textron Inc, has argued that Electronic Arts’ depiction of its helicopters in "Battlefield" was beyond fair use and amounted to a trademark infringement. EA preemptively went to court, suing Bell Helicopter to settle the issue.

The U.S. District Court, Northern District of California, has set a jury trial for the case in June.

Activision Warns of Rocky Second Half

Activision Blizzard Inc warned investors on Wednesday that it expects a challenging second-half and holiday quarter because of heavy competition and uncertainty around the launch of new video game consoles.

The shares of the largest U.S. video games publisher were down about 5 percent at $14.45 in after-hours trading from its $15.26 close on the Nasdaq.

Subscribers to "World of Warcraft," a large source of steady subscription-based revenue, dropped sharply by about 14 percent to 8.3 million last quarter from 9.6 million in the previous quarter, the company said.

Activision executives told analysts they expect Warcraft subscriber figures to dip further in coming months as the fantasy-action game continues to lose users to similar, free-to-play games.

"No one understands what ’numbers to go lower’ means and that’s got investors concerned," said Michael Pachter, an analyst at Wedbush Securities. "Activision’s going to have to stabilize that."

To arrest the loss of subscribers, the company will invest significantly in the franchise and deliver new content to engage players, Chief Executive Officer Bobby Kotick said in an interview.

The company, known for its "Call of Duty" and "Skylanders" games, slightly raised its 2013 revenue and earnings forecast to $4.25 billion and 82 cents per share, compared with $4.18 billion and 80 cents provided at the end of the last quarter ended January 30.

Its 2013 outlook was below the view of Wall Street analysts, who expected the company to forecast revenue of $4.27 billion and earnings at 85 cents per share.

In contrast, rival Electronic Arts Inc on Tuesday forecast fiscal 2014 earnings above Wall Street’s expectations, triggering a 17 percent rally in its shares on Wednesday.

The video game industry is grappling with flagging sales as players migrate from to buying packaged games for consoles to free or less-expensive offerings on mobile devices.

Moreover, consumers have held back from buying hardware and software as they await new versions of Sony Corp’s PlayStation and Microsoft Corp’s Xbox, which are expected later this year.

Nintendo Co Ltd’s new Wii U console, which was launched in November, has disappointed investors with its lackluster sales, casting doubt on the industry’s hope that new consoles could boost prospects.

This year, Activision will clash with a number of mega-franchises during the coming holidays, a crucial period that often accounts for the bulk of the industry’s annual revenue.

Its top releases include shooter game "Call of Duty: Ghosts", which will compete with EA’s "Battlefield 4" over the holidays. Its "Skylanders SWAP Force", a children’s fantasy-adventure game sold with actual toys that come to life onscreen, will battle Disney’s "Infinity", based on a similar concept, and is slated for release in August.

"Infinity is going to be supported by a large marketing budget so obviously, it’s something that’s formidable," Pachter said.

To try and get a leg up on the competition, Kotick told analysts that Activision will "further increase our sales and marketing investments," without offering specifics.

Activision’s warnings about the competition overshadowed strong first-quarter earnings.

The Santa Monica-based company said non-GAAP revenue, adjusted for the deferral of digital revenue and other items, rose to $804 million, surpassing Wall Street’s average revenue forecast for $704.6 million and up 37 percent from $587 million in the same quarter a year ago.

Non-GAAP income totaled $199 million, or 17 cents per share, in the fourth quarter, compared with $67 million, or 6 cents per share a year earlier. This beat Wall Street’s average earnings estimate of 11 cents per share, according to Thomson Reuters I/B/E/S.

Sony CEO, Executives Give Up Financial Bonuses

For years, Sony has suffered from lagging electronics sales and supporting new proprietary technology that simply hasn t panned-out on the market. While the PlayStation brand has long been one of Sony s strongest, and while Sony is now finally in the black, that doesn t mean the company doesn t want to become even more profitable following a significant bloodletting over the last couple of years.

According to The Raw Story (via Nikkei), 40 Sony executives   including well-known Sony CEO Kaz Hirai   are giving up their financial bonuses in a move described by a Sony spokeswoman as unprecedented. The move will only save Sony about $10 million (the company expects to make a profit of $403 million in fiscal year 2013), and is likely a largely symbolic move towards Sony s shareholders. Either way, it s a bigger move than last year, when seven Sony executives gave up their financial bonuses.

Sony will report its fiscal year 2013 results, running from March 2012 to March 2013, in early May.

=~=~=~=

A-ONE’s Headline News

The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Internet Sales Tax Bill Faces Tough Sell in House

Traditional retailers and cash-strapped states face a tough sell in the House as they lobby Congress to limit tax-free shopping on the Internet.

The Senate voted 69 to 27 Monday to pass a bill that empowers states to collect sales taxes from Internet purchases. Under the bill, states could require out-of-state retailers to collect sales taxes when they sell products over the Internet, in catalogs, and through radio and TV ads. The sales taxes would be sent to the states where a shopper lives.

Current law says states can only require retailers to collect sales taxes if the merchant has a physical presence in the state.

That means big retailers with stores all over the country like Wal-Mart, Best Buy and Target collect sales taxes when they sell goods over the Internet. But online retailers like eBay and Amazon don’t have to collect sales taxes, except in states where they have offices or distribution centers.

"This bill is about fairness," said Sen. Mike Enzi, R-Wyo., the bill’s main sponsor in the Senate. "It’s about leveling the playing field between the brick and mortar and online companies and it’s about collecting a tax that’s already due. It’s not about raising taxes."

The bill got bipartisan support in the Senate but faces opposition in the House, where some lawmakers regard it as a tax increase. Grover Norquist, the anti-tax advocate, and the conservative Heritage Foundation oppose the bill, and many Republicans have been wary of crossing them.

Supporters say the bill is not a tax increase. In many states, shoppers are required to pay unpaid sales tax when they file their state tax returns. However, states complain that few taxpayers comply.

"Obviously there’s a lot of consumers out there that have been accustomed to not having to pay any taxes, believing that they don’t have to pay any taxes," said Rep. Steve Womack, R-Ark., the bill’s main sponsor in the House. "I totally understand that, and I think a lot of our members understand that. There’s a lot of political difficulty getting through the fog of it looking like a tax increase."

On Tuesday morning, House Speaker John Boehner, R-Ohio, declined to say whether the House would take up the bill. Later, he told Bloomberg Television in an interview that he would "probably not" support the bill. But he said he would refer it to the House Judiciary Committee and "we’ll see what they think."

Rep. Bob Goodlatte, R-Va., chairman of the Judiciary Committee, said there are problems with the bill, but he did not reject it outright.

"While it attempts to make tax collection simpler, it still has a long way to go," Goodlatte said in a statement. Without more uniformity in the bill, he said, "businesses would still be forced to wade through potentially hundreds of tax rates and a host of different tax codes and definitions."

Goodlatte said he’s "open to considering legislation concerning this topic but these issues, along with others, would certainly have to be addressed."

Internet giant eBay led the fight against the bill in the Senate, along with lawmakers from states with no sales tax and several prominent anti-tax groups. The bill’s opponents say it would put an expensive obligation on small businesses because they are not as equipped as national merchandisers to collect and remit sales taxes at the multitude of state rates.

Businesses with less than $1 million in online sales would be exempt. EBay wants to exempt businesses with up to $10 million in sales or fewer than 50 employees.

"The contentious debate in the Senate shows that a lot more work needs to be done to get the Internet sales tax issue right, including ensuring that small businesses using the Internet are protected from new burdens that harm their ability to compete and grow," said Brian Bieron, eBay’s senior director of global public policy.

Some states have sales taxes as high as 7 percent, plus city and county taxes that can push the combined rate even higher.

Many governors   Republicans and Democrats   have been lobbying the federal government for years for the authority to collect sales taxes from online sales.

The issue is getting bigger for states as more people make purchases online. Last year, Internet sales in the U.S. totaled $226 billion, up nearly 16 percent from the previous year, according to government estimates.

States lost a total of $23 billion last year because they couldn’t collect taxes on out-of-state sales, according to a study done for the National Conference of State Legislatures, which has lobbied for the bill. About half of that was lost from Internet sales; half from purchases made through catalogs, mail orders and telephone orders, the study said.

Supporters say the bill makes it relatively easy for Internet retailers to comply. States must provide free computer software to help retailers calculate sales taxes, based on where shoppers live. States must also establish a single entity to receive Internet sales tax revenue, so retailers don’t have to send it to individual counties or cities.

Opponents worry the bill would give states too much power to reach across state lines to enforce their tax laws. States could audit out-of-state businesses, impose liens on their property and, ultimately, sue them in state court.

Senators Propose Law To Combat Cyber Theft

A group of senior Republican and Democratic senators proposed a new law on Tuesday to combat computer espionage and the theft of valuable commercial data from U.S. companies.

The four powerful senators - Democrats Carl Levin and Jay Rockefeller and Republicans John McCain and Tom Coburn - joined together to launch the Deter Cyber Theft Act.

The proposed law aims to combat the theft of intellectual property from U.S. companies, which spend billions in research and development only to be targeted by foreign firms and countries that illegally access their data and use it to compete against them.

General Keith Alexander, head of the U.S. National Security Agency and commander of the U.S. Cyber Command, has called the growing problem the "greatest transfer of wealth in history."

China is accused of being the biggest culprit in theft attempts against U.S. companies. American lawmakers have said U.S. companies suffered estimated losses in 2012 of more than $300 billion due to trade-secret theft, much of it due to Chinese cyber espionage.

Levin, chairman of the Armed Services Committee, said the new law would help protect American businesses and innovation.

"We need to call out those who are responsible for cyber theft and empower the president to hit the thieves where it hurts most - in their wallets, by blocking imports of products or from companies that benefit from this theft," Levin said in a statement.

McCain, a powerful voice in the Senate on armed services and foreign affairs issues, said the bill would give President Barack Obama authority to target those who try to benefit from cyber crime.

A divided U.S. Congress has not approved much legislation in recent years, given a string of partisan fiscal battles.

But with lawmakers on both sides of the political aisle acknowledging that cyber security is a rising concern, this bipartisan measure - sponsored by leading senators - will likely draw plenty of interest.

A senior Democratic aide described cyber security as a "huge priority," for Senate Majority Leader Harry Reid.

The proposed act would require the Director of National Intelligence to compile an annual report that includes a list of nations that engage in economic or industrial espionage in cyberspace against U.S. firms or individuals. It would include a priority watch list of the worst offenders.

The report would also include a list of U.S. technologies targeted by the espionage, details of what had been stolen and a list of items produced using the stolen information.

The DNI’s report would also list countries that had benefited from the theft and the action taken by the U.S. government to combat cyber espionage.

Under the proposed law, the president would be required to block imports of products containing stolen U.S. technology or products made by state-owned enterprises of nations on the DNI’s priority watch list that are similar to items identified as being made using stolen technology.

Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback

Even as the U.S. government confronts rival powers over widespread Internet espionage, it has become the biggest buyer in a burgeoning gray market where hackers and security firms sell tools for breaking into computers.

The strategy is spurring concern in the technology industry and intelligence community that Washington is in effect encouraging hacking and failing to disclose to software companies and customers the vulnerabilities exploited by the purchased hacks.

That’s because U.S. intelligence and military agencies aren’t buying the tools primarily to fend off attacks. Rather, they are using the tools to infiltrate computer networks overseas, leaving behind spy programs and cyber-weapons that can disrupt data or damage systems.

The core problem: Spy tools and cyber-weapons rely on vulnerabilities in existing software programs, and these hacks would be much less useful to the government if the flaws were exposed through public warnings. So the more the government spends on offensive techniques, the greater its interest in making sure that security holes in widely used software remain unrepaired.

Moreover, the money going for offense lures some talented researchers away from work on defense, while tax dollars may end up flowing to skilled hackers simultaneously supplying criminal groups. "The only people paying are on the offensive side," said Charlie Miller, a security researcher at Twitter who previously worked for the National Security Agency.

A spokesman for the NSA agreed that the proliferation of hacking tools was a major concern but declined to comment on the agency’s own role in purchasing them, citing the "sensitivity" of the topic.

America’s offensive cyber-warfare strategy - including even the broad outlines and the total spending levels - is classified information. Officials have never publicly acknowledged engaging in offensive cyber-warfare, though the one case that has been most widely reported - the use of a virus known as Stuxnet to disrupt Iran’s nuclear-research program - was lauded in Washington. Officials confirmed to Reuters previously that the U.S. government drove Stuxnet’s development, and the Pentagon is expanding its offensive capability through the nascent Cyber Command.

Stuxnet, while unusually powerful, is hardly an isolated case. Computer researchers in the public and private sectors say the U.S. government, acting mainly through defense contractors, has become the dominant player in fostering the shadowy but large-scale commercial market for tools known as exploits, which burrow into hidden computer vulnerabilities.

In their most common use, exploits are critical but interchangeable components inside bigger programs. Those programs can steal financial account passwords, turn an iPhone into a listening device, or, in the case of Stuxnet, sabotage a nuclear facility.

Think of a big building with a lot of hidden doors, each with a different key. Any door will do to get in, once you find the right key.

The pursuit of those keys has intensified. The Department of Defense and U.S. intelligence agencies, especially the NSA, are spending so heavily for information on holes in commercial computer systems, and on exploits taking advantage of them, that they are turning the world of security research on its head, according to longtime researchers and former top government officials.

Many talented hackers who once alerted companies such as Microsoft Corp to security flaws in their products are now selling the information and the exploits to the highest bidder, sometimes through brokers who never meet the final buyers. Defense contractors and agencies spend at least tens of millions of dollars a year just on exploits, which are the one essential ingredient in a broader cyber-weapons industry generating hundreds of millions annually, industry executives said privately.

Former White House cybersecurity advisors Howard Schmidt and Richard Clarke said in interviews that the government in this way has been putting too much emphasis on offensive capabilities that by their very nature depend on leaving U.S. business and consumers at risk.

"If the U.S. government knows of a vulnerability that can be exploited, under normal circumstances, its first obligation is to tell U.S. users," Clarke said. "There is supposed to be some mechanism for deciding how they use the information, for offense or defense. But there isn’t."

Acknowledging the strategic trade-offs, former NSA director Michael Hayden said: "There has been a traditional calculus between protecting your offensive capability and strengthening your defense. It might be time now to readdress that at an important policy level, given how much we are suffering."

The issue is sensitive in the wake of new disclosures about the breadth and scale of hacking attacks that U.S. intelligence officials attribute to the Chinese government. Chinese officials deny the allegations and say they too are hacking victims.

Top U.S. officials told Congress this year that poor Internet security has surpassed terrorism to become the single greatest threat to the country and that better information-sharing on risks is crucial. Yet neither of the two major U.S. initiatives under way - sweeping cybersecurity legislation being weighed by Congress and President Barack Obama’s February executive order on the subject - asks defense and intelligence agencies to spread what they know about vulnerabilities to help the private sector defend itself.

Most companies, including Microsoft, Apple Inc and Adobe Systems Inc, on principle won’t pay researchers who report flaws, saying they don’t want to encourage hackers. Those that do offer "bounties", including Google Inc and Facebook Inc, say they are hard-pressed to compete financially with defense-industry spending.

Some national-security officials and security executives say the U.S. strategy is perfectly logical: It’s better for the U.S. government to be buying up exploits so that they don’t fall into the hands of dictators or organized criminals.

When a U.S. agency knows about a vulnerability and does not warn the public, there can be unintended consequences. If malign forces purchase information about or independently discover the same hole, they can use it to cause damage or to launch spying or fraud campaigns before a company like Microsoft has time to develop a patch. Moreover, when the U.S. launches a program containing an exploit, it can be detected and quickly duplicated for use against U.S. interests before any public warning or patch.

Some losses occur even after a patch.

That happened to Microsoft and its customers with a piece of malicious software known as Duqu. Experts say it was designed to steal industrial-facility designs from Iran and that it used an exploit that tricked computers into installing malicious software disguised as a font to render type on the screen.

Those who dissected the program after its discovery in 2011 believe it was created by a U.S. agency. Though Duqu resembled Stuxnet in some respects, they couldn’t say for sure how it was assembled, or whether the spying tool had accomplished its mission.

What’s certain is that criminal hackers copied Duqu’s previously unheard-of method for breaking into computers and rolled it into "exploit kits," including one called Blackhole and another called Cool, that were sold to hackers worldwide.

Microsoft had by then issued a patch for the vulnerability. Nevertheless, hackers used it last year to attack 16 out of every 1,000 U.S. computers and an even greater proportion in some other countries, according to Finland-based security firm F-Secure.

The flaw became the second-most frequently tried among tens of thousands of known vulnerabilities during the second half of 2012, F-Secure said. Hackers installed a variety of malicious software in cases when the exploit worked, including copies of Zeus, a notorious program for stealing financial login information that has been blamed for hundreds of millions of dollars in bank thefts. Microsoft won’t say whether it has confronted U.S. officials about Duqu and other programs, but an executive said the company objects "to our products being used for malicious purposes."

Former NSA Director Hayden and others with high-level experience have boasted that U.S. offensive capabilities in cyberspace are the best in the world. But few outsiders had any idea what was possible before 2010, when a small laboratory discovered the worm called Stuxnet.

It took teams of security experts in several countries months to dissect the program. They discovered that it had been meticulously engineered to launch invisibly from a portable flash drive and spread through connected Windows-based personal computers in search of machines running a specific piece of industrial control software made by Siemens AG of Germany.

If Stuxnet found that software and a certain configuration, it changed some of the instructions in the program and hid its tracks. Eventually, the truth came out: The only place deliberately affected was an Iranian nuclear facility, where the software sped up and slowed down uranium-enriching centrifuges until they broke.

Stuxnet was unique in many ways, one of them being that it took advantage of four previously unknown flaws in Windows. In the industry, exploits of such vulnerabilities are called "zero-days," because the software maker has had zero days’ notice to fix the hole before the tool’s discovery.

It can take months for security patches to be widely installed after a vulnerability is reported, so even a "two-day" exploit, one released two days after a warning, is valuable.

But exploits can’t be counted on to work once the holes they rely on are disclosed. That means contractors are constantly looking for new ones that can be swapped in to a particular program after the original vulnerability is fixed. Some security firms sell subscriptions for exploits, guaranteeing a certain number per year.

"My job was to have 25 zero-days on a USB stick, ready to go," said a former executive at a defense contractor that bought vulnerabilities from independent hackers and turned them into exploits for government use.

Zero-day exploits will work even when the targeted software is up to date, and experts say the use of even a single zero-day in a program signals that a perpetrator is serious. A well-publicized hacking campaign against Google and scores of other companies in early 2010, attributed by U.S. officials and private experts to Chinese government hackers, used one zero-day.

Many zero-day exploits appear to have been produced by intelligence agencies. But private companies have also sprung up that hire programmers to do the grunt work of identifying vulnerabilities and then writing exploit code. The starting rate for a zero-day is around $50,000, some buyers said, with the price depending on such factors as how widely installed the targeted software is and how long the zero-day is expected to remain exclusive.

It’s a global market that operates under the radar, often facilitated by other companies that act as brokers. On the buy side are U.S. government agencies and the defense contractors that fold the exploits into cyber-weapons. With little or no regulation, it is impossible to say who else might be purchasing zero-days and to what end, but the customers are known to include organized crime groups and repressive governments spying on their citizens.

Even one of the four exploits used by Stuxnet may have been purchased. Swedish Defense Research Agency expert David Lindahl said the same trick employed by the exploit in question was used in a piece of Russian crime software called Zlob prior to Stuxnet’s discovery. The same person may have sold the exploit to both the United States and to Russian criminals. However, Lindahl and other experts said simultaneous invention can’t be ruled out.

The issue of rival countries or gangs using a flaw that U.S. officials have known about but decided to keep secret is a big concern. The National Security Agency declined to say whether or how often that happens, but researchers said simultaneous security discoveries occur often.

"It’s pretty naïve to believe that with a newly discovered zero-day, you are the only one in the world that’s discovered it," said Schmidt, who retired last year as the White House cybersecurity coordinator. "Whether it’s another government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long."

China is thought to do a lot of its work on exploits in-house, relying on its own programmers, though Reuters has reviewed email from self-declared

Chinese buyers offering large sums. "I really need some 0days,if you have some remote exploit 0days of windows system, I think I can buy it. you know, money is not the problem," one hopeful wrote in 2006.

Cesar Cerrudo, a researcher in Argentina and the recipient of the 2006 email, was among the first to sell zero-days in the open, targeting experts who wanted to test the security of networks for their employers or clients.

Cerrudo said he ignored some requests from China that seemed suspiciously detailed, such as one for an exploit for an out-of-date version of Microsoft Office. Cerrudo said he regrets selling to a research institution in Europe he won’t name that he later realized received a great deal of funding from a national government. Now Cerrudo works at IOActive Inc, a Seattle-based consulting firm that advises corporate clients on security.

"Fewer people are publishing details about vulnerabilities and exploits," Cerrudo said, and that hurts overall safety. "People are trying to keep their techniques and exploits private so they can make a lot of money."

A Paris-based security company called Vupen sells tools based on exploits to intelligence, law-enforcement and military authorities in most of the world. It refrains from selling to countries such as Iran or North Korea, and says it voluntarily follows European and U.S. rules limiting arms exports, though others say it isn’t clear whether exploits are subject to the most restrictive U.S. rules.

Until 2010, Vupen often notified software vendors for free when it found vulnerabilities, said chief executive Chaouki Bekrar. That has now changed. "As our research costs became higher and higher, we decided to no longer volunteer for multi-billion-dollar companies," Bekrar said. When software makers wouldn’t agree to a compensation system, he said, Vupen chose to sell to governments instead. "Software vendors created this market by not decently paying researchers for their hard work."

In Bekrar’s estimation, Vupen is doing good. "Exploits are used as part of lawful intercept missions and homeland security operations as legally authorized by law," he said, "to protect lives and democracies against both cyber and real world threats."

The company is one of the most visible players in the business. Vupen sent a dozen researchers to an elite April conference on offensive hacking techniques at the luxury Fontainebleau Hotel in Miami Beach, where attendees eschewed nametags, dined on stone crab and heard such talks as "Advanced Heap Manipulation in Windows 8." The only larger contingents were one from the conference’s organizer, zero-day reseller Immunity Inc, and one from the U.S. government.

A newer entrant to the market is ReVuln, based in Malta. ReVuln says it specializes in crafting exploits for industrial control systems that govern everything from factory floors to power generators.

This is a major concern for governments because such systems are considered prime targets for terrorists and enemy nations, with the potential for high loss of life. Additionally, the software that controls them is much harder to patch than something like Windows, which Microsoft frequently fixes with updates over the Internet. Employees at several large makers of control systems say they don’t know how to reach all their users, let alone convince them to make changes when holes are discovered.

ReVuln’s founders, Italian researcher Luigi Auriemma and former Research in Motion vulnerability hunter Donato Ferrante, declined to say anything about their customers. In an email interview, they said they sold some exploits exclusively and others more widely. Asked if they would be troubled if some of their programs were used in attacks that caused death or destruction, they said: "We don’t sell weapons, we sell information. This question would be worth asking to vendors leaving security holes in their products."

Much of the work on offensive cyber-warfare is done by publicly traded U.S. defense contractors, now joined by a handful of venture capital-backed start-ups seeking government buyers for a broad array of cyber-weapons that use exploits. Defense contractors both buy exploits and produce them in-house.

Major players in the field include Raytheon Co, Northrop Grumman Corp and Harris Corp, all of which have acquired smaller companies that specialize in finding new vulnerabilities and writing exploits. Those companies declined to discuss their wares. "It’s tough for us, when you get into the realm of offensive," said Northrop spokesman Mark Root.

Reuters reviewed a product catalogue from one large contractor, which was made available on condition the vendor not be named. Scores of programs were listed. Among them was a means to turn any iPhone into a room-wide eavesdropping device. Another was a system for installing spyware on a printer or other device and moving that malware to a nearby computer via radio waves, even when the machines aren’t connected to anything.

There were tools for getting access to computers or phones, tools for grabbing different categories of data, and tools for smuggling the information out again. There were versions of each for Windows, Apple and Linux machines. Most of the programs cost more than $100,000, and a solid operation would need several components that work together. The vast majority of the programs rely on zero-day exploits.

Intelligence agencies have a good reason to leave a lot of the spyware development work to outsiders, said Alex Stamos, chief technology officer at an Internet security unit of NCC Group Plc. "It’s just like munitions development," he said. "They don’t purchase it until the vendors can demonstrate it works."

Another newcomer with U.S. agencies as clients is Atlanta-based Endgame Inc, which in March raised $23 million in a second round of funding led by the blue-chip Silicon Valley venture capital firm Kleiner Perkins Caufield & Byers. Endgame is chaired by the chief executive of In-Q-Tel, a venture capital firm set up in 1999 at the request of the CIA to fund private companies developing technology that could be useful to the intelligence community.

Some of Endgame’s activities came to light in purloined emails published by hackers acting under the banner Anonymous. In what appear to be marketing slides, the company touted zero-day subscriptions as well as lists of exactly which computers overseas belonged to specific criminal "botnets" - networks of compromised machines that can be mobilized for various purposes, including stealing financial passwords and knocking websites offline with traffic attacks.

The point was not to disinfect the botnet’s computers or warn the owners.

Instead, Endgame’s customers in the intelligence agencies wanted to harvest data from those machines directly or maintain the ability to issue new commands to large segments of the networks, three people close to the company told Reuters.

Endgame declined to comment.

Ted Schlein, a Kleiner partner who sits on Endgame’s board, said he couldn’t comment on the company’s classified business. But he defended the idea of captive botnets.

"If you believe that wars are going to be fought in the world of cyber in the future, wouldn’t you want to believe you would have a cyber-army at your disposal? Why wouldn’t you want to launch a cyber-army if needed?"

Booming ’Zero-day’ Trade Has Washington Cyber Experts Worried

The proliferation of hacking tools known as zero-day exploits is raising concerns at the highest levels in Washington, even as U.S. agencies and defense contractors have become the biggest buyers of such products.

White House cybersecurity policy coordinator Michael Daniel said the trend was "very worrisome to us."

Asked if U.S. government buying in the offensive market was adding to the problem, Daniel said more study was needed. "There is a lot more work to be done in that space to look at the economic questions...so we can do a better job on the cost-benefit analysis," he said.

Some security experts say the government’s purchasing power could help instead of hurt. They argue the U.S. government should bring the market into the open by announcing it will pay top dollar for zero-days and then disclosing all vulnerabilities to the companies concerned and their customers.

"Given that people are now buying vulnerabilities, the U.S. should simply announce that it is cornering the market, that they will pay 10 times anyone else," said Dan Geer, chief information security officer at In-Q-Tel, the U.S. intelligence community’s venture capital firm. He said he was speaking outside of his official capacity.

Richard Clarke, who served as counter-terrorism chief in the White House before becoming a cybersecurity advisor there a decade ago, said the government should at least review the exploits it has and disclose the vast majority.

"In some rare cases, perhaps the government could briefly withhold that information in order to run a high-priority collection mission," he said. "Even then, however, the government should closely monitor to see if anyone else has discovered the vulnerability and begun to use it."

Howard Schmidt, who served as White House cybersecurity czar under Obama, said he agreed with Clarke’s approach. Asked if he had made the same argument during his recent two and a half years in the White House, he said he couldn’t betray confidences by going into detail.

But Schmidt added: "The entire discussion on cascading effects and the sort of unintended consequences of any type of malware was had more than once... That’s the discussion that needs to continue to take place."

Here’s One Way to Try to Avoid the FBI’s Internet Wiretapping Proposal

If The New York Times is to be believed, the Obama administration is "on the verge of" signing off on a proposal from the FBI that would make it easier for the agency’s to intercept online communications. Please allow us to offer a tip that may help you avoid the Feds’ steely gaze.

We should first explain what is being proposed. For some time, the FBI has sought a way to observe information that passes through internet service providers in the same way they can (with a warrant) listen in on phone conversations. The problem is that while it’s relatively easy for the FBI to deal with the handful of companies that operate telephone networks, there are many, many platforms on the Internet which people use to communicate: Gchat, Facebook, Twitter direct messages, Snapchat, etc. And as people   specifically, the people who the FBI wants to listen in on use phones less and the Internet more, less and less communication is visible to their wiretapping. In testimony before Congress in 2011, the FBI’s general counsel described what she called the "Going Dark" problem.

> [S]ome providers are currently obligated by law to have technical solutions in place prior to receiving a court order to intercept electronic communications, but do not maintain those solutions in a manner consistent with their legal mandate. Other providers have no such existing mandate and simply develop capabilities upon receipt of a court order. In our experience, some providers actively work with the government to develop intercept solutions, while others do not have the technical expertise or resources to do so. As a result, on a regular basis, the government is unable to obtain communications and related data, even when authorized by a court to do so.

The problem isn’t really encryption, as such. While communications over Facebook and GMail and Apple’s iMessage are encrypted, what the FBI really wants is a way for those companies   and others that don’t use encryption   to let it peek in on what is being said.

Not always, mind you   just after they get a court order. The FBI presents it as a natural evolution of its existing ability to eavesdrop on phone calls once a judge signs a warrant. In those cases, the FBI approaches a phone company, which allows access to communications involving a party. What the FBI wants to do, it assures those asking, is simply to allow that same sort of ability if it goes and knocks on Facebook’s front door, warrant in-hand. The Times quotes another of the FBI’s attorneys.

> This doesn t create any new legal surveillance authority, [Andrew Weissmann] said. This always requires a court order. None of the going dark solutions would do anything except update the law given means of modern communications.

Late last month, The Washington Post reported on the proposal being developed by a government task force which would need to be passed by Congress. The amendment to the existing wiretapping law   the Communications Assistance to Law Enforcement Act   would allow a court to impose a series of increasing fines if a firm won’t or can’t comply with an FBI request to allow it to observe communications. (In the past, the Feds would apparently back off from companies that resisted.) In addition to indicating the president’s likely support, The Times clarified how it would work in practice:

> Under the proposal, officials said, for a company to be eligible for the strictest deadlines and fines   starting at $25,000 a day   it must first have been put on notice that it needed surveillance capabilities, triggering a 30-day period to consult with the government on any technical problems.

Foreign-based communications services that do business in the United States would be subject to the same procedures, and would be required to have a point of contact on domestic soil who could be served with a wiretap order, officials said.

That notice that begins the 30-day requirement for compliance could, for example, be in the form of the signed warrant from the judge.

It sounds simple. It is not.

For one thing, internet communications are not like phone calls. While the FBI’s goal isn’t to break encryption directly, that’s its effect in practice. This is not a trivial endeavor. Internet traffic is encrypted at various levels of difficulty, some of which are far harder to access than others. In some cases, the encryption takes place between users and isn’t done by the company. Coming up with systems to allow the FBI access to communication could theoretically be very time- and resource-consuming. Because that cost is borne differently by companies of different sizes, The Times points out a strategy for those looking to evade observation.

> The difference [in the latest proposal], officials say, means that start-ups with a small number of users would have fewer worries about wiretapping issues unless the companies became popular enough to come to the Justice Department s attention.

Which brings us to the most obvious way for terrorists or drug dealers or law-breakers or, yes, privacy puritans to avoid the FBI’s proposed wiretapping ability: if you want to reduce the likelihood that your communications will be observed, check out what will hereafter be known as "burner" companies   new shops that enable the sort of communications you want to do but are unlikely to have enough users that one draws the attention of the FBI. Become a TechCrunch afficianado! When a company announces it’s "a new way to connect people," that’s your best bet, as long as it doesn’t become too popular. (The "burner" analogy to cheap cell phones   you’ve seen The Wire, right?   is flawed, of course; that would be more like creating new Facebook accounts to send messages for a day or so.)

But of course, the FBI is not the only who might have an easier time observing your communications if the proposal goes forward. Opponents argue that placing backdoors into online platforms, these companies will necessarily be creating a way for anyone with enough savvy and access (i.e. hackers) to discover and break in. The Verge quotes a professor from Columbia University: "I think it s a disaster waiting to happen.

There is a tiny chance that all of this is moot. The Guardian’s Glenn Greenwald pointed to a CNN interview last week with a former FBI agent who claimed that the federal government was already storing all digital communication. All as in all. This is highly unlikely, if only because of the infrastructure that would be required. But if it is the case: Go ahead and use Facebook.

U.S. Top Lawman Denies Bowing to Hollywood in Megaupload Case

The United States’ chief prosecutor has denied that its investigation into the Megaupload file-sharing site on charges of online piracy is an example of Washington bowing to Hollywood pressure.

During a visit to New Zealand, U.S. Attorney General Eric Holder also said that he saw no reason why Kim Dotcom, the founder of the defunct site who lives in New Zealand, should not be extradited to the United States to face charges of facilitating massive piracy of copyrighted music and movies.

"That’s not true," Holder told Radio New Zealand, when asked to respond to Dotcom’s claims that Hollywood moguls are pressuring Washington to target file-sharing sites, which can house pirated content uploaded and downloaded by individual users.

"(The case) was brought on the basis of facts, on the basis of law, and it is consistent with the enforcement priorities that this administration has had," he said.

The United States began a criminal copyright case against Dotcom in January 2012. At Washington’s request, New Zealand law enforcement officers conducted a dramatic raid on his mansion outside Auckland.

Attempts to have him sent to the United States for trial were delayed after a New Zealand court last year found that New Zealand used unlawful warrants in his arrest and illegally spied on him in the lead-up to the raid.

An extradition hearing is scheduled for August, although it could be delayed by further appeals. Holder said he expected Dotcom to be extradited to the United States, adding that he was happy with the level of cooperation with New Zealand authorities on the case.

"There are things which are working their way through the New Zealand court system, but we’ve had good communications, and I think at the end of the day, there will be an appropriate result," he said.

Dotcom and six associates face U.S. charges that they conspired to infringe copyrights, launder money and commit racketeering and fraud.

The copyright case could set a precedent for internet liability laws and, depending on its outcome, may force entertainment companies to rethink their distribution methods.

Dotcom maintains that Megaupload, which housed everything from family photos to Hollywood blockbusters, was merely a storage facility for online files, and should not be held accountable if content stored on the site was obtained illegally.

The U.S. Justice Department counters that Megaupload encouraged piracy by paying money to users who uploaded popular content and by deleting content that was not regularly downloaded.

Holder is visiting New Zealand this week for a meeting of attorneys general from the United States, New Zealand, Australia, Britain, and Canada.

Dutch Ponder Giving Police The Right To Hack

The Dutch government has unveiled the draft of a law that would give police investigating online crimes the right to hack into computers in the Netherlands or abroad and install spyware or destroy files.

Justice Minister Ivo Opstelten said Thursday that such actions would carried out only after the approval of a judge. The bill would also make it a crime for a suspect to refuse to decipher encrypted files during a police investigation.

Spokesman Wiebe Alkema said the bill will undergo revisions and be put to parliament by the end of the year.

Simone Halink of the digital rights group Bits of Freedom says the law would set a bad precedent, giving a "green light" to oppressive governments to hack into civilian computers.

Man Facing Charges Linked to SpyEye Virus

An Algerian man accused of helping to develop and market a computer program that drained millions of dollars from bank accounts around the world pleaded not guilty Friday to nearly two dozen charges.

A 23-count indictment charges Hamza Bendelladj, 24, with wire fraud, bank fraud, computer fraud and conspiracy. U.S. Attorney Sally Yates said the man was extradited to Atlanta from Thailand on Thursday and was arraigned in federal court Friday afternoon. A second person is also charged in the indictment but has not been identified. Investigators could not disclose whether the person was in the U.S. or abroad. Officials also could not disclose what information led them to Bendelladj.

Bendelladj, whose nickname is "Bx1," is accused of developing and marketing SpyEye, a banking Trojan. However, federal authorities have not said exactly how Bendelladj helped develop the software. Court records don’t indicate whether he had a lawyer.

The malware was implanted onto computers to secretly collect financial information and drain bank accounts. Authorities say the malware impacted 253 different financial institutions and is responsible for untold amounts of financial theft.

"We’re talking millions," Yates said Friday. "We don’t have the precise number quantified at this point."

Trojans such as SpyEye can be profitable for cybercriminals. A small group of hackers in Eastern Europe arrested in 2010 was able to steal about $70 million from companies, municipalities and churches in Europe and the U.S.

SpyEye was designed to automatically steal sensitive information   such as bank account credentials, credit card information, passwords and PIN numbers   after being implanted in victims’ computers. After the program took control of a computer, it allowed hackers to use a number of covert techniques to trick victims into giving up their personal information including data grabbing and presenting victims with a fake bank account page. The information was then relayed to a command and control server, which was used to access bank accounts.

Bendelladj was indicted in December 2011 and was on a trip from Malaysia to Egypt when he was arrested during a layover at an airport in Bangkok on Jan. 5, 2013. Police there seized two laptops, a tablet computer, a satellite phone and external hard drives.

Although authorities say he never set foot on U.S. soil, Bendelladj is accused of leasing a virtual server from an unidentified Internet company in Atlanta to control computers that were impacted by SpyEye. The company was unaware the man was allegedly using the server for illegal purposes, Yates said.

"The federal indictment and extradition of Bendelladj should send a very clear message to those international cybercriminals who feel safe behind their computers in foreign lands that they are, in fact, within reach," Mark F. Giuliano of the FBI’s Atlanta field office said in a news release.

Bendelladj and others allegedly developed and sold various versions of SpyEye and its components on the Internet between 2009 and 2011. Cybercriminals were able to customize their purchases to choose specific methods of gathering personal information from victims. Bendelladj and others also allegedly advertised SpyEye on Internet forums focused on cybercrime and other criminal activity.

Yates said that Bendelladj is not accused of being part of a specific criminal organization, and that he and his associates are not accused of carrying out cyberterrorism.

While the arrest does show that authorities are vigilant about trying to fight cybercrime, cybersecurity experts said there is still a vast network of cybercriminals finding more sophisticated ways to remain anonymous and create malware resistant to antivirus programs.

"At the end of the day, this one arrest, unfortunately, won’t cause a lot of reduction in online fraud attempts," said George Tubin, senior security strategist at Boston-based Trusteer, a provider of cybercrime prevention programs. "Hopefully it sends a message maybe to the fraudsters that you can be caught and you need to think twice."

Investigators say SpyEye is still active, and authorities are trying to track down computer hackers who are still using the virus. Hackers have developed a mobile version of SpyEye called Spitmo, which targets victims’ smartphones, Tubin said. Cybercriminals can steal personal information through victims’ computers and forward themselves text messages from the victims’ cellphones to fraudulently verify the person’s identity and lock them out of bank accounts and other personal accounts. That method is more widely used in Europe, Tubin said.

If convicted, Bendelladj faces up to 30 years in prison for conspiracy to commit wire and bank fraud, and up to five years for conspiracy to commit computer fraud. The 21 counts of wire and computer fraud carry maximum sentences of between five and 20 years each. The man may also be fined up to $14 million.

Acer Aspire R7: Windows 8 Laptop-Tablet In One Crazy Package

Ever since Windows 8 was announced last year a slew of crazy-looking computers have been introduced. Take Lenovo’s IdeaPad Yoga laptop, which has a screen that rotates all the way around to turn into a tablet. Or Asus’ Taichi with its two screens, which allow you to use the device as a laptop and then close the lid to make it a tablet.

But Acer has just upped the ante in the funky Windows 8 computer game. Today, at an event in New York City, the company introduced the Aspire R7, a full-fledged 15.6-inch laptop with a "floating" screen. The screen hinge allows the touchscreen to be propped up and then angled, like a desktop monitor or all-in-one computer. You can then even flip the touchscreen around, so if a person is sitting across the table they can see it. The idea, Acer says, is that all the touchscreen Windows 8 laptops are awkward to use - you have to reach out over the keyboard and trackpad. This brings the screen closer to you.

Speaking of the keyboard and trackpad, Acer decided that putting the trackpad below the keyboard was just a bit too traditional. On the R7 it put the trackpad above of the keyboard so that when the screen is folded down you can still use the keyboard.

Acer will begin selling the R7 on May 17 for $1,000. Best Buy will carry a special "Star Trek Into Darkness" version, which will come with a free download of the "Star Trek: The Video Game." The laptop comes standard with a 15.6-inch 1920 x 1080-resolution screen, a Core i5 processor, 6GB of RAM, and a combo 500 GB hard drive with a 24 GB solid-state drive.

Last month it was reported that the PC market has seen the steepest decline in its history. Research firm IDC’s data showed that shipments of PCs plunged 14 percent in the first quarter of this year. That’s the sharpest decline in sales of personal computers since the firm started tracking the industry in 1994. Technology experts and pundits have hypothesized about the causes of the ailing personal computer market. IDC, specifically, cited Windows 8, Microsoft’s new computer and tablet operating system, as one of the main reasons people turned away from buying computers.

"While some consumers appreciate the new form factors and touch capabilities of Windows 8, the radical changes to the UI, removal of the familiar Start button, and the costs associated with touch have made PCs a less-attractive alternative to dedicated tablets and other competitive devices," Bob O’Donnell, IDC Program Vice President, said in a statement last month.

Acer, however, doesn’t seem to be too worried about that. In addition to the Aspire R7, it released the Aspire P3, an "ultrabook convertible," or a Windows 8 tablet with a detachable keyboard dock. It is available now, starting at $799.99.

Common Windows 8 Gripes and Possible Solutions

Microsoft is preparing an update to Windows 8 for release later this year. It says the changes are designed to address complaints and confusion with the new operating system.

Windows 8 is the most radical overhaul of Microsoft’s operating system since Windows 95 came out nearly two decades ago. It was revamped to embrace the types of touch-screen controls popular on smartphones and tablet computers, devices that are siphoning sales from the desktop and laptop PCs that have been Microsoft’s traditional stronghold. Windows 8 was released with much fanfare in October, but got a lukewarm reception from consumers.

Part of the problem is that Windows 8 tries to be all things to all people. It’s designed to respond to touch-screen controls, but it also works with traditional mouse and keyboard commands. It offers a new layout that resembles tablet computers, but it also has a desktop mode that looks like previous versions of Windows. What results is confusion.

In addition, many of the controls to launch programs and change settings have been tucked away. That gives Windows 8 a cleaner look, but it also requires people to do more work finding all the controls.

Microsoft Corp. isn’t saying much about what the new Windows 8 will have. Nor will it say whether it will charge for the upgrade. What the Redmond, Wash., company will say is that it’s responding to customer feedback in developing the update.

Here’s a look at some of that feedback and possible solutions in the coming update:

The problem: There’s no central place for launching programs and changing settings.

Windows 8 features a new start page that takes over the entire screen. The page is filled with boxes, or tiles, for accessing your favorite programs. But to get to programs you use less often, you need to slide up a menu from the bottom, click on "All apps" and find the one you want. When you’re already using a program, such as a Web browser, you have to switch back to this start page to launch a different one, even if it’s one of your favorites. To access settings, you need to slide over a set of icons, known as charms, from the right of the screen.

By contrast, past versions of Windows have a "start" button on the lower left corner, which allowed quick access to programs and settings without interrupting your workflow. That button is always there as you move from program to program.

The solution: Restore the "start" button. Don’t make people figure out where everything is. Make it easy for them to see where to "start."

The problem: Microsoft is encouraging people to use the new tablet-style layout filled with tiles, but many programs are designed for the older, desktop mode. That’s the case even with Microsoft’s popular Office suite of business tools, despite the fact that the latest version of Office came out months after Windows 8 comes out.

As a result, using Windows 8 feels like running two different computers on the same machine, as the tile and desktop modes don’t communicate well with each other. Consider Microsoft’s Internet Explorer 10 browser. Web pages you open in desktop mode won’t appear when you switch to the browser in the tile mode. Because many popular programs run only in desktop mode, it would make sense to do most of your computing there, but Windows 8 always forces you into tile mode when you start the machine.

The solution: Allow people to enter the desktop mode automatically when they start their machines. Over time, people may get more comfortable with tile mode and may want to switch, but don’t force it on them and make them resent it before they are ready.

The problem: Those charms on the right are useful for restarting your machine, configuring your wireless connection and changing other settings. But you’re left to figure out how to access them. On touch screens, you have to know to swipe a menu from the right, like opening a sock drawer. If you’re using a mouse, you need to drag the cursor to the top or bottom right of the screen, then drag it to the appropriate charm.

The solution: Besides restoring the "start" button and having those settings instantly accessible, offer an option to have that sock drawer continually appear. It’s similar to how the Taskbar is always present on older versions of Windows, usually at the bottom. It’s also similar to how the Dock is always there on Mac computers (though once you’re used to it, you can hide the Dock until you move your cursor there).

The problem: There’s no obvious way to close programs, the way you can by hitting an "x’’ at the corner of the program in older versions of Windows. You need to figure out how to drag the app to the bottom of the screen, and the way you do it depends on whether you are using touch or a mouse. Stray too far to the left or the right, and your computer will enter a multi-window mode instead.

The solution: Restore the "x." Don’t force people to do gestures that don’t seem intuitive to the task at hand.

The problem: In making it easy for touch screens, mouse and keyboard commands are more complex to use and figure out.

The solution: Don’t try to be a one-size-fits-all operating system. Apple and Google have kept their systems separate for touch-screen mobile devices and for traditional computers that use mouse or trackpad controls.

Microsoft can improve usability by designing the operating system for one or the other. Don’t expect this to change in the promised update, though.

IT Industry Backs Software Patent Change

The Government has announced a change to planned new patent rules today which has put an end to fears that computer software might be covered by new patent protection.

Industry sources have welcomed the decision and the Labour Party has called it "a humiliating back down".

Commerce Minister Craig Foss has released a supplementary order paper to clarify issues around the patentability of computer programmes in the

Patents Bill.

"These changes ensure the Bill is consistent with the intention of the Commerce Select Committee recommendation that computer programs should not be patentable," Foss said.

The Patents Bill is designed to replace the Patents Act 1953 and update the New Zealand patent regime.

The Commerce Select Committee recommended in 2010 that software should not be patentable, which led to lobbying from patent lawyers and others.

Foss then released a supplementary order paper (SOP) which changed some wording in the bill and caused industry concern that he might be reversing his decision.

Ongoing consultation with the New Zealand software and IT sector had led to today’s announcement, Foss said.

"I’m confident we’ve reached a solution where we can continue to protect genuine inventions and encourage Kiwi businesses to export and grow."

The Labour Party said Foss had been forced into "a humiliating back down" over the software patent system.

"Last year Craig Foss gave in to patent lawyers and multinational software players and sought to impose a software patents system on our IT sector," said communications and IT spokesperson Clare Curran.

"He overrode the advice of the Commerce Select Committee that copyrighting software would smother innovation."

Foss said there had been "a lot of noise" about the SOP when he released it and today’s move was not a back-down.

"There were some concerns out there but that was a misconception about what we intended from the first SOP."

His intention was always that devices such as digital cameras or washing machines, that make use of a computer program, would be patentable, but not the software itself, Foss said.

Internet New Zealand welcomed today’s tabling of the SOP, saying it made clear that computer software was not patentable in New Zealand.

Foss’ decision to amend the Patents Bill drew to a close "years of wrangling between software developers, ICT players and multinational heavyweights over the vexed issue of patentability of software", said spokesperson Susan Chalmers

"Patenting software would not only make the continued development of the Internet more difficult, it would reduce innovation and could well stymie interoperability of various software platforms," she said.

New Zealand’s largest IT representative body, the Institute of IT Professionals, expressed relief and said a major barrier to software-led innovation had been removed.

Chief executive Paul Matthews said although there were varied opinions on the matter, the consensus amongst professionals was that the patent system simply did not work for software.

"If you look at the New Zealand market, you would be hard pressed to find many people that were thinking patents would be a good idea."

It was in New Zealand’s best interests for software to continue to be covered through the provisions of copyright - "a far more appropriate mechanism" - in the same way movies and books were, Matthews said.

"We believe it’s near impossible for software to be developed without breaching some of the hundreds of thousands of software patents awarded around the world, often for ’obvious’ work.

"Thus many software companies in New Zealand, creating outstanding and innovative software, live with a constant risk that their entire business could be threatened due to litigious action by a patent holder."

Patenting software would give large overseas firms the opportunity to monopolise a concept and crush smaller competitors through the legal system, he said.

New Zealand’s biggest software exporter, Orion Health, also welcomed Foss’ decision.

Chief executive Ian McCrae said obvious things were being patented under the current regime.

"You might see a logical enhancement to your software, but you can’t do it because someone else has a patent.

"In general, software patents are counter-productive, often used obstructively and get in the way of innovation."

Matthews said a recent poll of more than 1000 Kiwi IT professionals found 94 per cent wanted to see software patents gone.

A petition launched by the industry against software patents received over 1,000 signatures in under a week, he said.

Tavi Leads the Teens-Are-Dumb-on-Twitter Revolt Against Dumb Adults

Today the teens are giving adults a taste of their own medicine on Twitter. In response to the ongoing #followateen movement, in which grownups examine the tweets of kids to discover how silly most of Twitter is, teens on the social platform are rising up and asking their brethren to #followanadult   because, as the team behind one prominent teems claims, adults are lame, too. If this all sounds like a bunch of gibberish   it kind of is!   we’re here to explain.

The idea for #followateen goes back to 2011 and is credited to Boston Phoenix music writer David Thorpe, a.k.a. @Arr. And the concept is pretty simple: Go on Twitter. Follow a teen who uses Twitter. Tweet about what they do on Twitter with the hashtag #followateen. Thorpe explained all of this in an email to BuzzFeed’s Katie Notopolous back in April: "If you get below the surface, Twitter is like 99% teens who are mad at their moms and think English class is total bullshit (and don’t even get me started about Keighlinn, who is being a TOTAL bitch). It’s a lot of fun to find a random one and casually keep tabs on their stupid teen life. It’s not a stalky thing, it’s just about tuning in to the weird secret worldwide teenosphere and seeing what’s up with today’s youth."

In April Thorpe tweeted:

> By request of @katienotopoulos, let’s bring back #followateen for 2013. Here’s how it works: find a teen, follow it, and report on its life.
>
> Lucrative Trillion (@Arr) April 12, 2013

So Notopolous, quite a few BuzzFeed employees, and other Internet denizens have been keeping tabs on teens. Just yesterday, Notopolous published an update on #followateen, with some examples of what various young people have been up to on social media. Said young people, it seems, have pretty mundane lives:

> My teen wants a smoothie and hates everyone.#followateen
>
> Juston Payne (@justonpayne) May 2, 2013

> My teen got asked to prom by dude texting "prom??".. It was very cute #followateen
>
> Cam Cam (@squidvstractor) April 30, 2013

The #followateen movement has not gone without criticism. An essay in The New Inquiry by Helena Fitzgerald focused on the creepiness of it all:

> Besides the comments on proms and crushes and parents and school and #yolo, the most common theme on #followateen is people pointing out that #followateen is creepy. It s a good point. Of course it s creepy. It s really creepy. If you haven t yet noticed, Twitter is, itself, creepy.

But today some Internent-dwelling teens are trying to turn the tables. This morning, Rookie, the website aimed at teenage girls that is the brainchild of teenage wunderkind fashion blogger/Internet celebrity Tavi Gevinson, tweeted:

> Growns who think teen tweets are dumb (#followateen) should see their fellow adults’. Today we dare to #followanadult. Join us won’t you?
>
> Rookie (@RookieMag) May 3, 2013

Now of course Gevinson is a particularly Internet-savvy teenager, and not exactly #followateen’s target audience. Anaheed Alani, Rookie’s editorial director (and an adult herself) told The Atlantic Wire in an email that the the idea for #followanadult came from a discussion on Facebook last night: "Something about it felt off to us   mostly that the tweets the people who took part in that were mocking were no lamer than most adults’ tweets. A writer of ours, Hazel Cills, came up with the idea for #followanadult and made the first tweet about it." Cills, who has been tweeting things like "My adult works in media and hates New York #followanadult," explained her reasoning in an email to the Wire as well:

> I remember seeing a lot of #followateen tags on my Twitter feed and thinking that was kind of weird and sort of mocking teens. The #followanadult tag is kind of like teens saying "Okay adults, we see you, we’ll let you know how unintentionally hilarious you are too." I follow mostly adults already, so all of my tweets are composites of a bunch of adults I follow. I don’t think the tag is really a parody, rather it’s turning that followateen tag back on its creators in a really funny way.

Gevinson, herself, has also been participating:

> my adult is making yet another hilarious joke about google vs bing #followanadult
> Tavi Gevinson (@tavitulle) May 3, 2013

> my adult is offended by alleged misuse of the word "literally" #followanadult
> Tavi Gevinson (@tavitulle) May 3, 2013

And others have joined in:

> my adult is having anxiety because Joran van der Sloot will be out of jail in 28 years. #followanadult
> rahima (@afdalxrahima) May 3, 2013

Given that this is all very insular, there are also some adults who just want to be followed.

So what is all this? It’s part social experiment, part inside joke, part amusing Internet ephemera turned on its head. Here’s what it looks like, if your head isn’t spinning:

Cern Re-creating First Web Page To Revere Early Ideals Comments

A team at the European Organisation for Nuclear Research (Cern) has launched a project to re-create the first web page.

The aim is to preserve the original hardware and software associated with the birth of the web.

The world wide web was developed by Prof Sir Tim Berners-Lee while working at Cern.

The initiative coincides with the 20th anniversary of the research centre giving the web to the world.

> I want my children to be able to understand the significance of this point in time: the web is already so ubiquitous - so, well, normal - that one risks failing to see how fundamentally it has changed

According to Dan Noyes, the web manager for Cern’s communication group, re-creation of the world’s first website will enable future generations to explore, examine and think about how the web is changing modern life.

"I want my children to be able to understand the significance of this point in time: the web is already so ubiquitous - so, well, normal - that one risks failing to see how fundamentally it has changed," he told BBC News.

"We are in a unique moment where we can still switch on the first web server and experience it. We want to document and preserve that".

The hope is that the restoration of the first web page and web site will serve as a reminder and inspiration of the web’s fundamental values.

At the heart of the original web is technology to decentralise control and make access to information freely available to all. It is this architecture that seems to imbue those that work with the web with a culture of free expression, a belief in universal access and a tendency toward decentralising information.

Subversive

It is the early technology’s innate ability to subvert that makes re-creation of the first website especially interesting.

While I was at Cern it was clear in speaking to those involved with the project that it means much more than refurbishing old computers and installing them with early software: it is about enshrining a powerful idea that they believe is gradually changing the world.

I went to Sir Tim’s old office where he worked at Cern’s IT department trying to find new ways to handle the vast amount of data the particle accelerators were producing.

I was not allowed in because apparently the present incumbent is fed up with people wanting to go into the office.

But waiting outside was someone who worked at Cern as a young researcher at the same time as Sir Tim. James Gillies has since risen to be Cern’s head of communications. He is occasionally referred to as the organisation’s half-spin doctor, a reference to one of the properties of some sub-atomic particles.

Amazing dream

Mr Gillies is among those involved in the project. I asked him why he wanted to restore the first website.

"One of my dreams is to enable people to see what that early web experience was like," was the reply.

"You might have thought that the first browser would be very primitive but it was not. It had graphical capabilities. You could edit into it straightaway. It was an amazing thing. It was a very sophisticated thing."

Continue reading the main story

> One of my dreams is to enable people to see what that early web experience was like... It was an amazing thing

Those not heavily into web technology may be sceptical of the idea that using a 20-year-old machine and software to view text on a web page might be a thrilling experience.

But Mr Gillies and Mr Noyes believe that the first web page and web site is worth resurrecting because embedded within the original systems developed by Sir Tim are the principles of universality and universal access that many enthusiasts at the time hoped would eventually make the world a fairer and more equal place.

The first browser, for example, allowed users to edit and write directly into the content they were viewing, a feature not available on present-day browsers.

Ideals eroded

And early on in the world wide web’s development, Nicola Pellow, who worked with Sir Tim at Cern on the www project, produced a simple browser to view content that did not require an expensive powerful computer and so made the technology available to anyone with a simple computer.

According to Mr Noyes, many of the values that went into that original vision have now been eroded. His aim, he says, is to "go back in time and somehow preserve that experience".

"This universal access of information and flexibility of delivery is something that we are struggling to re-create and deal with now.

"Present-day browsers offer gorgeous experiences but when we go back and look at the early browsers I think we have lost some of the features that Tim Berners-Lee had in mind."

Mr Noyes is reaching out to ask those who were involved in the NeXT computers used by Sir Tim for advice on how to restore the original machines.

Awe

The machines were the most advanced of their time. Sir Tim used two of them to construct the web. One of them is on show in an out-of-the-way cabinet outside Mr Noyes’s office.

I told him that as I approached the sleek black machine I felt drawn towards it and compelled to pause, reflect and admire in awe.

"So just imagine the reaction of passers-by if it was possible to bring the machine back to life," he responded, with a twinkle in his eye.

The initiative coincides with the 20th anniversary of Cern giving the web away to the world free.

> Keeping the web free and freely available is almost a human right

There was a serious discussion by Cern’s management in 1993 about whether the organisation should remain the home of the web or whether it should focus on its core mission of basic research in physics.

Sir Tim and his colleagues on the project argued that Cern should not claim ownership of the web.

Management agreed and signed a legal document that made the web publicly available in such a way that no one could claim ownership of it and that would ensure it was a free and open standard for everyone to use.

Mr Gillies believes that the document is "the single most valuable document in the history of the world wide web".

He says: "Without it you would have had web-like things but they would have belonged to Microsoft or Apple or Vodafone or whoever else. You would not have a single open standard for everyone."

The web has not brought about the degree of social change some had envisaged 20 years ago. Most web sites, including this one, still tend towards one-way communication. The web space is still dominated by a handful of powerful online companies.

But those who study the world wide web, such as Prof Nigel Shadbolt, of Southampton University, believe the principles on which it was built are worth preserving and there is no better monument to them than the first website.

"We have to defend the principle of universality and universal access," he told BBC News.

"That it does not fall into a special set of standards that certain organisations and corporations control. So keeping the web free and freely available is almost a human right."

=~=~=~=

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.